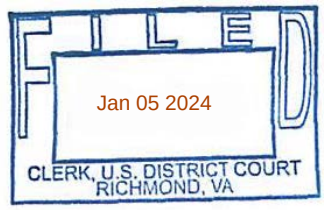
AO 106 (Rev. 04/10) Application for a Search Warrant

UNITED STATES DISTRICT COURT

for the

Eastern District of Virginia



In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)

(a) the person of John David Cutlip; (b) electronic devices on the person or in the possession of John David Cutlp; and (c) 756 Canterbury Drive, Ruther Glen, Virginia 22546

Case No. 3:24-sw-3

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location)*:
See Attachment A, fully incorporated by reference herein.

located in the Eastern District of Virginia, there is now concealed *(identify the person or describe the property to be seized)*:
See Attachment B, fully incorporated by reference herein.

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☑ contraband, fruits of crime, or other items illegally possessed;
- ☑ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 U.S.C. §§ 2252A(a)(2); 2252A(a)(5)	Distribution or Receipt of Child Pornography; Possession of Child Pornography

The application is based on these facts:
See attached affidavit, fully incorporated by reference herein.

- ☑ Continued on the attached sheet.
- ☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Reviewed by AUSA/SAUSA:

Kashan K. Pathan, Assistant U.S. Attorney
Printed name and title

Applicant's signature

Matthew Marasco, FBI Special Agent
Printed name and title

Sworn to before me and signed in my presence.

Date: 01/05/2024

/s/
Judge's signature

City and state: Richmond, VA

Hon. Summer L. Speight, U.S. Magistrate Judge
Printed name and title

IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF VIRGINIA
Richmond Division

IN THE MATTER OF THE SEARCH OF: (a) THE PERSON OF JOHN DAVID CUTLIP; (b) ELECTRONIC DEVICES ON THE PERSON OR IN THE POSSESSION OF JOHN DAVID CUTLIP; AND (c) 756 CANTERBURY DRIVE, RUTHER GLEN, VIRGINIA 22546	Case No. 3:24-sw-3

AFFIDAVIT IN SUPPORT OF AN APPLICATION UNDER RULE 41 FOR A WARRANT TO SEARCH AND SEIZE

I, Matthew Marasco, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant authorizing the search of the person of JOHN DAVID CUTLIP (hereinafter, "CUTLIP"), as further described in Attachment A-1; electronic devices on the person or in the possession of CUTLIP; and the premises located at 756 Canterbury Drive, Ruther Glen, Virginia 22546 (hereinafter, "PREMISES") as further described in Attachment A-2. In particular, this affidavit is made in support of an application for a warrant to search for and seize evidence, instrumentalities, and fruits of violations of 18 U.S.C. § 2252A(a)(2) (Distribution or Receipt of Child Pornography) and 18 U.S.C. § 2252A(a)(5) (Possession of Child Pornography), as further described in Attachment B.

2. I am a Special Agent with the Federal Bureau of Investigation (FBI), United States Department of Justice, and have been since September 2019. I am assigned to the Richmond Field

Office of the FBI in Richmond, Virginia, and am responsible for conducting investigations pertaining to child exploitation. As part of my duties, I have received training regarding the investigation of federal crimes including crimes against children, human trafficking, civil rights, and public corruption. By virtue of my employment with the FBI, I have performed a variety of investigative tasks including, but not limited to, conducting arrests and executing federal search warrants. As a Special Agent, I am an investigative or law enforcement officer within the meaning of 18 U.S.C. § 2510(7).

3. The facts in this affidavit come from my personal observations and review of records, my training and experience, and information obtained from other agents and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all my knowledge about this matter.

RELEVANT STATUTORY PROVISIONS

4. **Distribution or Receipt of Child Pornography:** 18 U.S.C. § 2252A(a)(2) provides that it is a crime to knowingly receive or distribute any child pornography that has been mailed, or, using any means or facility of interstate or foreign commerce, shipped or transported in or affecting interstate or foreign commerce by any means, including by computer.

5. **Possession of Child Pornography**: 18 U.S.C. § 2252A(a)(5) provides that it is a crime to knowingly possess, or knowingly access with intent to view, any child pornography that has been mailed, or shipped or transported using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce by any means, including by computer, or that was produced using materials that have been mailed, or shipped or transported in or affecting interstate or foreign commerce by any means, including by computer.

6. **Child pornography or Child abusive material** means any visual depiction, in any format, of sexually explicit conduct where: (A) the production involves the use of a minor engaging

in sexually explicit conduct; (B) such visual depiction is a digital or computer-generated image that is substantially indistinguishable from that of a minor engaged in sexually explicit conduct; or (C) such visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaged in sexually explicit conduct. *See* 18 U.S.C. § 2256(8).

7. **Visual depictions** include undeveloped film and videotape, and data stored on computer disk or by electronic means, which are capable of conversion into a visual image, and data which are capable of conversion into a visual image that has been transmitted by any means, whether or not stored in a permanent format. *See* 18 U.S.C. § 2256(5).

8. **Minor** means any person under the age of eighteen years. *See* 18 U.S.C. § 2256(1).

9. **Sexually explicit conduct** means actual or simulated: (i) sexual intercourse, including genital-genital, oral-genital, or oral-anal, whether between persons of the same or opposite sex; (ii) bestiality; (iii) masturbation; (iv) sadistic or masochistic abuse; or (v) lascivious exhibition of the genitals or pubic area of any person. *See* 18 U.S.C. § 2256(2).

TECHNICAL TERMS

10. Based on my training and experience, I use the following technical terms to convey the following meanings:

a. **Computer**, as used herein, is defined pursuant to 18 U.S.C. § 1030(e)(1) as "an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical or storage functions and includes any data storage facility or communications facility directly related to or operating in conjunction with such device."

b. **Storage Medium**: A storage medium is any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

c. **Wireless Telephone**: A wireless telephone (or mobile telephone, or cellular telephone) is a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional "land line" telephones. A wireless telephone usually contains a "call

log," which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include storing names and phone numbers in electronic "address books;" sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may also include global positioning system ("GPS") technology for determining the location of the device.

d. **Smartphone:** A portable personal computer with a mobile operating system having features useful for mobile or handheld use. Smartphones, which are typically pocket-sized (as opposed to tablets, which are larger in measurement), have become commonplace in modern society in developed nations. While the functionality of smartphones may vary somewhat from model to model, they typically possess most if not all of the following features and capabilities: 1) place and receive voice and video calls; 2) create, send and receive text messages; 3) voice-activated digital assistants (such as Siri, Google Assistant, Alexa, Cortana, or Bixby) designed to enhance the user experience; 4) event calendars; 5) contact lists; 6) media players; 7) video games; 8) GPS navigation; 9) digital camera and digital video camera; and 10) third-party software components commonly referred to as "apps." Smartphones can access the Internet through cellular as well as Wi-Fi ("wireless fidelity") networks. They typically have a color display with a graphical user interface that covers most of the front surface of the phone and which usually functions as a touchscreen and sometimes additionally as a touch-enabled keyboard.

e. **SIM Card**: Stands for a "subscriber identity module" or "subscriber identification module," which is the name for an integrated circuit used in mobile phones that is designed to securely store the phone's international mobile subscriber identity (IMSI) number and its related key, which are used to identify and authenticate subscribers on mobile telephony devices (such as mobile phones and computers). It is also possible to store contact information on many SIM cards.

f. **Log Files**: Records automatically produced by computer programs to document electronic events that occur on computers. Computer programs can record a wide range of events including remote access, file transfers, logon/logoff times, and system errors. Logs are often named based on the types of information they contain. For example, web logs contain specific information about when a website was accessed by remote computers; access logs list specific information about when a computer was accessed from a remote location; and file transfer logs list detailed information concerning files that are remotely transferred.

g. **Internet**: A global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

h. **Internet Protocol Address (IP address)**: A unique number used by a computer to access the Internet. Every computer attached to the Internet computer must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static–that is, long-term–IP addresses, while other computers have dynamic that is, frequently changed–IP addresses. Internet providers use either IP version 4 or more recently IP version 6. IPv4 is a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). IPv4 is composed of 32-bit address length and is the fourth version of the Internet Protocol (IP). IPv6 is composed of 128-bit address length and is the latest updated version of the Internet Protocol (IP). Given the rapid growth of the volume of internet-enabled devices over the past two decades, in early 2011, the Internet Assigned Numbers Authority exhausted the global IPv4 free pool. As such, many providers switched to IPv6, which is a series of eight hexadecimal digits, each separated by colons (e.g., FFE:FFFF:7654:FEDA:1245:BA98:3210:4562).

i. The terms "**records**," "**documents**," and "**materials**," as used herein, include all information recorded in any form, visual or aural, and by any means, whether in handmade form (including, but not limited to, writings, drawings, painting), photographic form (including, but not limited to, microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, photocopies), mechanical form (including, but not limited to, phonograph records, printing, typing) or electrical, electronic or magnetic form (including, but not limited to, tape recordings, cassettes, compact discs, electronic or magnetic storage devices such as floppy diskettes, hard disks, CD-ROMs, digital video disks ("DVDs"), Personal Digital Assistants ("PDAs"), Multi Media Cards ("MMCs"), memory sticks, optical disks, printer buffers, smart cards, memory calculators, electronic dialers, or electronic notebooks, as well as digital data files and printouts or readouts from any magnetic, electrical or electronic storage devices).

COMPUTERS, ELECTRONIC STORAGE, AND FORENSIC ANALYSIS

11. As described above and in Attachment B, this application seeks permission to search for records that might be found on CUTLIP's person, devices found on his person or in his possession, and on the PREMISES, in whatever form they are found. The warrant applied for would authorize the seizure of electronic storage media or, potentially, the copying of electronically stored information, all under Rule 41(e)(2)(B).

12. **Probable Cause:** I submit that if a computer or storage medium is found on the PREMISES, there is probable cause to believe those records will be stored on that computer or storage medium, for at least the following reasons:

a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space - that is, in space on the storage medium that is not currently being used by an active file - for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

c. Wholly apart from user-generated files, computer storage media - in particular, computers' internal hard drives - contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory "swap" or paging files. Computer users typically do not erase or delete this evidence, because special software is typically

required for that task. However, it is technically possible to delete this information.

d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache."

13. **Forensic Evidence:** As further described in Attachment B, this application seeks permission to locate not only computer files that might serve as direct evidence of the crimes described on the warrant, but also for forensic electronic evidence that establishes how computers were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence will be on any storage medium in the PREMISES because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created, although this information can later be falsified.

b. As explained herein, information stored within a computer and other electronic storage media may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United

States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, information stored within a computer or storage media (e.g., registry information, communications, images and movies, transactional information, records of session times and durations, internet history, and anti-virus, spyware, and malware detection programs) can indicate who has used or controlled the computer or storage media. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. The existence or absence of anti-virus, spyware, and malware detection programs may indicate whether the computer was remotely accessed, thus inculpating or exculpating the computer owner. Further, computer and storage media activity can indicate how and when the computer or storage media was accessed or used. For example, as described herein, computers typically contain information that logs computer user account session times and durations, computer activity associated with user accounts, electronic storage media that connected with the computer, and the IP addresses through which the computer accessed networks and the internet. Such information allows investigators to understand the chronological context of computer or electronic storage media access, use, and events relating to the crime under investigation. Additionally, some information stored within a computer or electronic storage media may provide crucial evidence relating to the physical location of other evidence and the suspect. For example, images stored on a computer may both show a particular location and have geolocation information incorporated into its file data. Such file data typically also contains information indicating when the file or image was created. The

existence of such image files, along with external device connection logs, may also indicate the presence of additional electronic storage media (e.g., a digital camera or cellular phone with an incorporated camera). The geographic and timeline information described herein may either inculpate or exculpate the computer user. Last, information stored within a computer may provide relevant insight into the computer user's state of mind as it relates to the offense under investigation. For example, information within the computer may indicate the owner's motive and intent to commit a crime (e.g., internet searches indicating criminal planning), or consciousness of guilt (e.g., running a "wiping" program to destroy evidence on the computer or password protecting/encrypting such evidence in an effort to conceal it from law enforcement).

c. A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about how computers were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, computer evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a computer was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

14. **Necessity of Seizing or Copying Entire Computers or Storage Media:** In most cases, a thorough search of a premises for information that might be stored on storage media often requires the seizure of the physical storage media and later off-site review consistent with the warrant. In lieu of removing storage media from the premises, it is sometimes possible to make an image copy of storage media. Generally speaking, imaging is the taking of a complete electronic picture of the computer's data, including all hidden sectors and deleted files. Either seizure or imaging is often necessary to ensure the accuracy and completeness of data recorded on the storage media, and to prevent the loss of the data either from accidental or intentional destruction. This is true because of the following:

a. *The time required for an examination.* As noted above, not all evidence takes the form of documents and files that can be easily viewed on site. Analyzing evidence of how a computer has been used, what it has been used for, and who has used it requires considerable time, and taking that much time on premises could be unreasonable. As explained above, because the warrant calls for forensic electronic evidence, it is exceedingly likely that it will be necessary to thoroughly examine storage media to obtain evidence. Storage media can store a large volume of information. Reviewing that information for things described in the warrant can take weeks or months, depending on the volume of data stored, and would be

impractical and invasive to attempt on-site.

b. *Technical requirements.* Computers can be configured in several different ways, featuring a variety of different operating systems, application software, and configurations. Therefore, searching them sometimes requires tools or knowledge that might not be present on the search site. The vast array of computer hardware and software available makes it difficult to know before a search what tools or knowledge will be required to analyze the system and its data on the Premises. However, taking the storage media off-site and reviewing it in a controlled environment will allow its examination with the proper tools and knowledge.

c. *Variety of forms of electronic media.* Records sought under this warrant could be stored in a variety of storage media formats that may require off-site reviewing with specialized forensic tools.

15. **Nature of Examination**: Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of electronic devices, including cellular telephones, consistent with the warrant. The examination may require techniques, including, but not limited to, computer-assisted scans of the entire medium, that might expose many parts of a hard drive to human inspection to determine whether it is evidence described by the warrant.

16. Because several people share the PREMISES as a residence, it is possible that the PREMISES will contain storage media that are predominantly used, and perhaps owned, by persons who are not suspected of a crime. If agents nonetheless reasonably believe that the things described in this warrant could be found on any of those computers or storage media, the warrant applied for would permit the seizure and review of those items as well.

CHARACTERISTICS OF COLLECTORS OF CHILD PORNOGRAPHY

17. Based upon my knowledge, experience, and training in child pornography investigations, and the training and experience of other law enforcement officers with whom I have had discussions, there are certain characteristics common to individuals involved in the collection of child pornography (hereinafter referred to as "collectors").

18. Collectors may receive sexual stimulation and satisfaction from contact with children, or from having fantasies of children engaged in sexual activity or suggestive poses, or from literature describing such activity.

19. Collectors may collect sexually explicit or suggestive materials in a variety of media, including photographs, magazines, motion pictures, videotapes, books, slides, drawings, and/or other visual media. Collectors typically use these materials for their own sexual arousal and gratification. Collectors often have companion collections of child erotica. Child erotica are materials or items that are sexually suggestive and arousing to pedophiles, but which are not in and of themselves obscene or pornographic. Such items may include photographs of clothed children, drawings, sketches, fantasy writings, diaries, pedophilic literature, and sexual aids.

20. Collectors who also actively seek to engage in sexual activity with children may use these materials to lower the inhibitions of a child they are attempting to seduce, convince the child of the normalcy of such conduct, sexually arouse their selected child partner, or demonstrate how to perform the desired sexual acts.

21. Collectors almost always possess and maintain their "hard copies" of child pornographic images and reference materials (e.g., mailing and address lists) in a private and secure location. With the growth of the internet and computers, many collections are maintained in digital format. Typically, these materials are kept at the collector's residence for easy access and viewing. Collectors usually place high value on their materials because of the difficulty, and

the legal and social danger, associated with acquiring them. As a result, it is not uncommon for collectors to retain child pornography for long periods, even for years. Collectors often discard child pornography images only while "culling" their collections to improve their overall quality.

22. Collectors also may correspond with and/or meet others to share information and materials. They may save correspondence from other child pornography distributors/collectors, including contact information like email addresses, and may conceal such correspondence as they do their sexually explicit material.

23. Collectors prefer not to be without their child pornography for any prolonged periods of time. This behavior has been documented by law enforcement officers involved in the investigation of child pornography throughout the world.

24. Subscribers to websites that are primarily designed to provide child pornography have a strong likelihood of being collectors of child pornography. This high degree of correlation between subscription and collection behavior has been repeatedly confirmed during nationwide law enforcement initiatives.

25. In sum, collectors of child pornography frequently maintain their collections in a private and secure location such as their residence, often in digital format, for long periods of time. They also maintain information related to their receipt or distribution of such media in that location, including correspondence with and contact information for other individuals distributing or sharing child pornography.

PROBABLE CAUSE

26. Between January 2023 and February 2023, an Online Covert Employee (OCE) in the FBI Tampa Field Office communicated with an identified male subject via the online social media platform "Kik", owned and operated by MediaLab, Inc. The subject expressed the desire to

engage in sexual activity with the OCE's fictitious 14-year-old male child and distributed child sexual abuse material (CSAM) to the OCE during the communications. Ultimately, the subject drove to Seminole County, Florida on February 1, 2023, and was arrested by law enforcement.

27. A search warrant was obtained for the subject's cellular telephone, and a forensic review of the phone revealed multiple communications between the subject and male juveniles between 12 and 17 years old during which the subject solicited the juveniles for sexual acts. Additionally, multiple images and videos of CSAM were located on the phone, as well as evidence he distributed and received CSAM via Kik messages and group chats.

28. One such group chat was identified as "Sexy Taboo." The group chat appeared to be for individuals who have a sexual attraction to children based on the conversation contained within the chat. The chat was initiated on January 15, 2023 and remained active at least until the subject's arrest on February 1, 2023.

29. Kik user Johnforfun269 was one of the participants in the Sexy Taboo group chat. As CSAM is distributed within the chat, Johnforfun269 actively participates in the conversation. For example, on one occasion on January 17, 2023, another user in the chat states, "Everyone hear [sic] into young." In response, Johnforfun269 replied, "Yes." In another exchange on the same day, a different user states, "Kids are made for us men to fuck." Johnforfun269 replied, "Damn right."

30. Approximately 11 CSAM images and videos are transmitted in the chat. The images and videos depict what appear to be children engaged in a variety of sexual acts. For instance, one video of approximately 24 seconds in length depicts a prepubescent minor female in a pink shirt and nude from the waist down lying on her back on an orange surface. During the video, an unknown male is engaging in anal sex with the minor female.

31. Pursuant to an administrative subpoena, on March 6, 2023, MediaLab, Inc. provided the following information associated with Kik user Johnforfun269:

Kik username: Johnforfun269
Name: John Smith
Email: jcutlip69@gmail.com.

Additionally, MediaLab, Inc. provided a list of IP addresses associated with the account, including 160.19.10.177 on February 2, 2023 at 12:53:00 UTC.

32. Pursuant to an administrative subpoena, on May 8, 2023, VA Skywire, LLC provided information associated with IP address 160.19.10.177 on February 2, 2023 at 12:53:00 UTC, which resolves to Palmer's Creek Apartments located at 5111 High Rock Road, Fredericksburg, Virginia 22407, operated by Bonaventure Property Management Services, LLC.

33. In August 2023, the FBI Tampa Field Office forwarded the above information to the FBI Richmond Field Office for additional investigation.

34. Queries of open source and law enforcement databases identified JOHN DAVID CUTLIP, date of birth (DOB) xx/xx/1969, Social Security Number XXX-XX-1893, address 756 Canterbury Drive, Ruther Glen, VA 22546, telephone number 540-809-0129 as the individual likely associated with Kik account Johnforfun269. CULTIP's employment records indicate he has been employed by Bonaventure Property Management Services, LLC since 2022.

35. Pursuant to an administrative subpoena, on September 8, 2023, Verizon Wireless provided the following information for the account associated with telephone number 540-809-0129:

Subscriber Name: John Cutlip
Subscriber Address: 756 Canterbury Drive, Ruther Glen, VA 22546
Home Phone: 540-548-4500
Work Phone: 540-548-4500
Account Number: 620536248-1
Active Since: 7/21/2006

36. Pursuant to a Federal Grand Jury subpoena, on October 10, 2023, Google LLC provided the following information for the account associated with email address jcutlip69@gmail.com:

Google Account ID: 274901837124
Name: john cutlip
Given Name: john
Family Name: cutlip
e-Mail: jcutlip69@gmail.com
Recovery SMS: +15408090129 [US]

37. Pursuant to an administrative subpoena, on October 24, 2023, MediaLab, Inc. provided an additional list of IP addresses associated with Kik account johnforfun269, including the following:

IP Address 174.216.184.46, Port 10257, on 1/15/2023 at 15:12:04 UTC

IP Address 174.206.98.134, Port 11689, on 1/17/2023 at 19:39:02 UTC

IP Address 174.206.97.103, Port 6459, on 1/18/2023 at 12:36:22 UTC

IP Address 174.206.108.82, Port 1495, on 1/21/2023 at 03:11:38 UTC

IP Address 174.206.99.254, Port 2223, on 1/22/2023 at 01:45:54 UTC

IP Address 174.193.83.142, Port 13511, on 1/27/2023 at 05:51:43 UTC

IP Address 174.193.83.25, Port 4085, on 1/29/2023 at 03:53:04 UTC

38. Pursuant to a Federal Grand Jury subpoena, on November 13, 2023, Verizon Wireless identified the above IP addresses provided by Medialab, Inc as corresponding to telephone number 540-809-0129. The telephone number 540-809-0129 was previously identified as belonging to CUTLIP with a listed address of the PREMISES.

BIOMETRIC ACCESS TO DEVICES

39. This warrant permits law enforcement agents to obtain from the person of JOHN DAVID CUTLIP the display of any physical biometric characteristics (such as fingerprint/thumbprint or facial characteristics) necessary to unlock any devices requiring such biometric access subject to seizure pursuant to this warrant. The grounds for this request are as follows:

40. I know from my training and experience, as well as from information found in publicly available materials published by device manufacturers, that many electronic devices, particularly newer mobile devices and laptops, offer their users the ability to unlock the device through biometric features in lieu of a numeric or alphanumeric passcode or password. These biometric features include fingerprint scanners, facial recognition features, and iris recognition features. Some devices offer a combination of these biometric features, and the user of such devices can select which features they would like to utilize.

41. If a device is equipped with a fingerprint scanner, a user may enable the ability to unlock the device through his or her fingerprints. For example, Apple offers a feature called "Touch ID," which allows a user to register up to five fingerprints that can unlock a device. Once a fingerprint is registered, a user can unlock the device by pressing the relevant finger to the device's Touch ID sensor, which is found in the round button (often referred to as the "home" button) located at the bottom center of the front of the device. The fingerprint sensors found on devices produced by other manufacturers have different names but operate similarly to Touch ID.

42. If a device is equipped with a facial-recognition feature, a user may enable the ability to unlock the device through his or her face. For example, this feature is available on certain Android devices and is called "Trusted Face." During the Trusted Face registration process, the user holds the device in front of his or her face. The device's front-facing camera then analyzes

and records data based on the user's facial characteristics. The device can then be unlocked if the front-facing camera detects a face with characteristics that match those of the registered face. Facial recognition features found on devices produced by other manufacturers (such as Apple's "Face ID") have different names but operate similarly to Trusted Face.

43. If a device is equipped with an iris-recognition feature, a user may enable the ability to unlock the device with his or her irises. For example, on certain Microsoft devices, this feature is called "Windows Hello." During the Windows Hello registration, a user registers his or her irises by holding the device in front of his or her face. The device then directs an infrared light toward the user's face and activates an infrared-sensitive camera to record data based on patterns within the user's irises. The device can then be unlocked if the infrared-sensitive camera detects the registered irises. Iris-recognition features found on devices produced by other manufacturers have different names but operate similarly to Windows Hello.

44. In my training and experience, users of electronic devices often enable the aforementioned biometric features because they are considered to be a more convenient way to unlock a device than by entering a numeric or alphanumeric passcode or password. Moreover, in some instances, biometric features are considered to be a more secure way to protect a device's contents. This is particularly true when the users of a device are engaged in criminal activities and thus have a heightened concern about securing the contents of a device.

45. As discussed in this Affidavit, your Affiant has reason to believe that one or more digital devices will be found during the search. The passcode or password that would unlock the device(s) subject to search under this warrant currently is not known to law enforcement. Thus, law enforcement personnel may not otherwise be able to access the data contained within the

device(s), making the use of biometric features necessary to the execution of the search authorized by this warrant.

46. I also know from my training and experience, as well as from information found in publicly available materials including those published by device manufacturers, that biometric features will not unlock a device in some circumstances even if such features are enabled. This can occur when a device has been restarted, inactive, or has not been unlocked for a certain period of time. For example, Apple devices cannot be unlocked using Touch ID or Face ID when (1) more than 48 hours has elapsed since the device was last unlocked or (2) when the device has not been unlocked using a fingerprint for 4 hours *and* the passcode or password has not been entered in the last 156 hours. Biometric features from other brands carry similar restrictions. With Apple devices, a passcode will be required if the phone has five failed attempts to unlock via Face ID. This is often reached by simply handling the phone during arrest or evidence inventory. In addition to device restart as mentioned above, the passcode will also be required after remote activation lock, or when the side or power buttons are pressed for longer than two seconds placing the phone in Emergency SOS mode. Thus, in the event law enforcement personnel encounter a locked device equipped with biometric features, the opportunity to unlock the device through a biometric feature may exist for only a short time.

47. Due to the foregoing, if law enforcement personnel encounter any device(s) that are subject to seizure pursuant to this warrant and may be unlocked using one of the aforementioned biometric features, this warrant permits law enforcement personnel to obtain from the aforementioned person the display of any physical biometric characteristics (such as fingerprint/thumbprint or facial characteristics) necessary to unlock any device(s), including to (1) press or swipe the fingers (including thumbs) of the aforementioned person(s) to the fingerprint

scanner of the device(s) found at the PREMISES or on CUTLIP's person; (2) hold the device(s) found at the PREMISES or on CUTLIP's person in front of the face of the aforementioned person(s) to activate the facial recognition feature; and/or (3) hold the device(s) found at the PREMISES or on CUTLIP's person in front of the face of the aforementioned person(s) to activate the iris recognition feature, for the purpose of attempting to unlock the device(s) in order to search the contents as authorized by this warrant. The proposed warrant does not authorize (nor does it prohibit) law enforcement to request that the aforementioned person state or otherwise provide the password or any other means that may be used to unlock or access the device(s). Moreover, the proposed warrant does not authorize (nor does it prohibit) law enforcement to ask the aforementioned person to identify the specific biometric characteristics (including the unique finger(s) or other physical features) that may be used to unlock or access the device(s). That is, if agents in executing the warrant ask any of the aforementioned person for the password to any device(s), or to identify which biometric characteristic unlocks any device(s), the agents will not state or otherwise imply that the warrant requires such person to provide such information; that is, the agents will make clear that any such request is voluntary/the person is free to refuse the request.

* * * * *

CONCLUSION

48. Based on the forgoing, I submit there is probable cause to believe that CUTLIP has committed violations of 18 U.S.C. §§ 2252A(a)(2) (Distribution or Receipt of Child Pornography) and 2252A(a)(5) (Possession of Child Pornography). I further submit that probable cause exists to search (i) the person of CUTLIP, as further described in Attachment A-1, (ii) any electronic devices found on CUTLIP's person and/or in CUTLIP's possession, and (iii) the PREMISES, as further described in Attachment A-2, for evidence and instrumentalities of violations of 18 U.S.C. §§ 2252A(a)(2) (Distribution or Receipt of Child Pornography) and 2252A(a)(5) (Possession of Child Pornography), as further described in Attachment B.

Respectfully submitted,

Matthew Marasco
Special Agent
FBI Richmond Field Office

SUBSCRIBED and SWORN before me this 5th day of January 2024.

/s/

Honorable Summer L. Speight
United States Magistrate Judge

ATTACHMENT A-1

Property to Be Searched

The person to be searched is JOHN DAVID CUTLIP, a male born in xx/xx/1969, with brown hair and approximately 5'7" tall, including all personal items and containers, including electronic devices, in his physical possession, on his person, or in areas within his immediate control.

ATTACHMENT A-2

Property to Be Searched

The property to be searched is 756 Canterbury Drive, Ruther Glen, Virginia 22546 (the "PREMISES"). The PREMISES is a multi-story, single-family residential structure located in Caroline County, within the Eastern District of Virginia.

ATTACHMENT B

Particular Things to be Seized

1. All records relating to violations of 18 U.S.C. §§ 2252A(a)(2) (Distribution or Receipt of Child Pornography) and 2252A(a)(5) (Possession of Child Pornography), including, but not limited to, the following:

   a. Any and all visual depictions of minors;

   b. Any and all address books, names and lists of names and addresses of minors;

   c. Any and all records reflecting physical contacts, whether real or imagined, with minors;

   d. Any and all child erotica, including photographs of children that are not sexually explicit, drawings, sketches, fantasy writings, diaries, and sexual aids; and

   e. Any and all communications and correspondence – in whatever form, digital or physical – concerning the distribution, receipt, and/or possession of child pornography.

2. Computers, electronic devices, or storage media used as a means to commit the violations described above.

3. For any computer, electronic devices, or storage medium whose seizure is otherwise authorized by this warrant, and any computer or storage medium that contains or in which is stored records or information that is otherwise called for by this warrant (hereinafter, "COMPUTER"):

   a. Evidence of who used, owned, or controlled the COMPUTER at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondences;

   b. Evidence of software that would allow others to control the COMPUTER, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

   c. Evidence of the lack of such malicious software;

   d. Evidence of the attachment to the COMPUTER of other storage devices or similar containers for electronic evidence;

   e. Evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the COMPUTER.

f. Evidence of the times the COMPUTER was used;

g. Passwords, encryption keys, and other access devices that may be necessary to access the COMPUTER;

h. Documentation and manuals that may be necessary to access the COMPUTER or to conduct a forensic examination of the COMPUTER;

i. Records of or information about Internet Protocol addresses used by the COMPUTER;

j. Records of, or information about, the COMPUTER's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses;

k. Contextual information necessary to understand the evidence described in this attachment.

During the execution of the search of the CUTLIP's person and the PREMISES, as further described in Attachments A-1 and A-2, law enforcement personnel are also specifically authorized to obtain from CUTLIP the compelled display of any physical biometric characteristics (such as fingerprint/thumbprint, facial characteristics, or iris display) necessary to unlock any device(s) requiring such biometric access subject to seizure pursuant to this warrant for which law enforcement has reasonable suspicion that the aforementioned person's physical biometric characteristics will unlock the device(s), to include pressing fingers or thumbs against and/or putting a face before the sensor, or any other security feature requiring biometric recognition of:

(a) any device(s) found at the PREMISES or on CUTLIP's person,
(b) where the device(s) are limited to those which are capable of containing and reasonably could contain fruits, evidence, information, contraband, or instrumentalities of the offense(s) as described in the search warrant affidavit and warrant Attachments A-1 and A-2,

for the purpose of attempting to unlock the device(s)'s security features in order to search the contents as authorized by this warrant.

While attempting to unlock the device by use of the compelled display of biometric characteristics pursuant to this warrant, law enforcement is not authorized to demand that the aforementioned person state or otherwise provide the password or identify the specific biometric characteristics (including the unique finger(s) or other physical features), that may be used to unlock or access the device(s). Nor does the warrant authorize law enforcement to use the fact that the warrant allows law enforcement to obtain the display of any biometric characteristics to compel the aforementioned person to state or otherwise provide that information. However, the voluntary disclosure of such information by the aforementioned person is permitted. To avoid confusion on that point, if agents in executing the warrant ask any of the aforementioned person for the password to any device(s), or to identify which biometric characteristic (including the unique finger(s) or other physical features) unlocks any device(s), the agents will not state or otherwise imply that the warrant requires the person to provide such information, and will make clear that providing any such information is voluntary and that the person is free to refuse the request.

This warrant authorizes a review of electronically stored information, communications, other records, and information disclosed pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the FBI may deliver a complete copy of the disclosed electronic data to the custody and control of attorneys for the government and their support staff for their independent review.

If the government identifies seized materials, that are potentially attorney-client privileged or subject to the work product doctrine ("protected materials"), the Prosecution Team,

which consists of law enforcement agents, investigators, analysts, attorneys for the government, and personnel designated by an attorney for the government who are involved in the investigation and prosecution of any cases relating to this search warrant, will discontinue review until a Filter Team of government attorneys and agents is established. The Filter Team will have no previous or future involvement in the investigation of this matter, and the Filter Team's work must be overseen and supervised by an Assistant United States Attorney. The Filter Team will review all seized communications and segregate potentially protected materials, i.e. communications to/from an attorney, or that otherwise reference or reflect attorney advice. At no time will the Filter Team advise the Prosecution Team of the substance of any of the potentially protected materials. The Filter Team will seek further guidance from the Magistrate Judge issuing the warrant with respect to obtaining a court order or other authorization before providing any potentially protected materials to the Prosecution Team. After review and subject to the direction of supervising attorneys, the Filter Team then will provide all communications that are not potentially protected materials to the Prosecution Team and the Prosecution Team may resume its review. If the Filter Team decides that any of the potentially protected materials are not protected (e.g., the communication includes a third party or the crime-fraud exception applies), the Filter Team must obtain either agreement from defense counsel/counsel for the privilege holder or a court order before providing these potentially protected materials to the Prosecution Team.

Your affiant requests the search warrant for the aforementioned items to include the opening and searching of any locked safes, boxes, and compartments.